МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

ЕСТЕСТВЕННОНАУЧНЫЙ ФАКУЛЬТЕТ
Кафедра «Информатика и ИТ»

«Утверждаю»
Декан естественнонаучного факультета
_____ Лещукович А.И.
«_1_» Сентября___2026 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по учебной дисциплине (модулю)

БЕЗОПАСНОСТЬ МОБИЛЬНЫХ УСТРОЙСТВ

Направление подготовки – 10.03.01 «Информационная безопасность»
Профиль – Безопасность компьютерных систем
(по отрасли или в сфере профессиональной деятельности)
Форма подготовки - очная
Уровень подготовки – бакалавриат

ДУШАНБЕ 2026

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ

Код компетенции	Результаты освоения ОПОП	Перечень планируемых результатов обучения	Вид оценочного знания
УК-2	**Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы ихрешения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений**	**ИУК-2.1.** Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение. **ИУК-2.2.** Определяет ресурсное обеспечение для достижения поставленной цели; **ИУК-2.3.** Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **ИУК-2.4.** Выполняет задачи в рамках своей ответственности в соответствии с запланированными результатами, при необходимости корректирует способы решения задач	Отчеты по практическим работам. Устный опрос. Презентация
ПК-2	**Способент разрабатывать и адаптиро-вать прикладное программное обеспечение**	**ИПК-2.1.** Применяет современные технологии разработки и адаптации прикладного программного обеспечения **ИПК-2.2.** Участвует в разработке на современных языках программирования и адаптации прикладного программного обеспечения **ИПК-2.3.** Применяет современные технологии для разработки веб-приложений	Отчеты по практическим работам. Устный опрос. Презентация
ПК-3	**Способен проектировать информационные системы по видам обеспечения**	**ИПК-3.1.** Применяет элементы технологий проектирования информационных систем; осуществляет и обосновывает выбор проектных решений по видам обеспечения информационных систем **ИПК-3.2.** Участвует в проектировании экономических информационных систем или их частей (модулей)	Отчеты по практическим работам. Устный опрос. Презентация

ТЕМЫ РЕФЕРАТОВ И ПИСЬМЕННЫХ РАБОТ
(рефератов, письменных работ)

1. Понятие безопасности WEB-приложений.
2. Архитектура WEB-приложений и её влияние на безопасность.
3. Основные угрозы безопасности WEB-приложений.
4. Модель угроз для WEB-приложений.
5. Уязвимости аутентификации пользователей.
6. Уязвимости авторизации и управления доступом.
7. Управление сессиями в WEB-приложениях.
8. Риски небезопасной обработки пользовательского ввода.
9. SQL-инъекции и причины их возникновения.
10. Межсайтовый скриптинг (XSS).

11. Межсайтовая подделка запросов (CSRF).
12. Уязвимости при загрузке и обработке файлов.
13. Ошибки конфигурации WEB-приложений и серверов.
14. Угрозы утечки данных в WEB-приложениях.
15. Использование HTTPS и его роль в безопасности.
16. Безопасность хранения учетных данных пользователей.
17. Хэширование и защита паролей.
18. Уязвимости сторонних библиотек и компонентов.
19. Безопасность API WEB-приложений.
20. Атаки отказа в обслуживании (DoS/DDoS).
21. Логирование и аудит безопасности WEB-приложений.
22. Тестирование безопасности WEB-приложений.
23. Роль пентестинга в обеспечении WEB-безопасности.
24. Программные средства защиты WEB-приложений.
25. Современные тенденции безопасности WEB-приложений.

Критерии оценки выполнения самостоятельной работы.

В основу разработки балльно рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется постоянно в процессе его обучения в университете. Настоящая система оценки успеваемости студентов основана на использовании совокупности контрольных точек, равномерно расположенных на всем временном интервале изучения дисциплины. При этом предполагается разделение всего курса на ряд более или менее самостоятельных, логически завершенных блоков и модулей и проведение по ним промежуточного контроля.

Студентам выставляются следующие баллы за выполнение задания к ПК:

- **оценка «отлично» (10 баллов):** контрольные тесты, а также самостоятельно выполненные семестровые задания, выполненные полностью и сданные в срок в соответствии с предъявляемыми требованиями;

- **оценка «хорошо» (8-9 баллов):** задание выполнено и в целом отвечает предъявляемым требованиям, но имеются отдельные замечания в его оформлении или сроке сдачи;

- **оценка «удовлетворительно» (6-7 баллов):** задание выполнено не до конца, отсутствуют ответы на отдельные вопросы, имеются отклонения в объеме, содержании, сроке выполнения;

- **оценка «неудовлетворительно» (5 и ниже):** отсутствует решение задачи, задание переписано (скачано) из других источников, не проявлена самостоятельность при его выполнении.

Текущий контроль осуществляется в ходе учебного процесса по результатам выполнения самостоятельной работы и контрольной работы.

Основными формами текущего контроля знаний являются:

- обсуждение вынесенных в планах практических занятий лекционного материала и контрольных вопросов;

- решение тестов и их обсуждение с точки зрения умения сформулировать выводы, вносить рекомендации и принимать адекватные управленческие решения;

- выполнение контрольной работы и обсуждение результатов;

- участие в дискуссиях в качестве участника и модератора групповой дискуссии по темам дисциплины;

- написание и презентация доклада;

- написание самостоятельной (контрольной) работы.

Для контроля усвоения данной дисциплины учебным планом предусмотрен экзамен. Общее количество баллов по дисциплине - 100 баллов. Распределение баллов на текущий и промежуточный контроль при освоении дисциплины, а также итоговой оценке представлено ниже.

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

по дисциплине

«БЕЗОПАСНОСТЬ WEB-ПРИЛОЖЕНИЙ»:

1. Сущность и задачи безопасности мобильных устройств.
2. Основные угрозы и риски мобильной безопасности.
3. Уязвимости мобильных операционных систем.
4. Вредоносное ПО для мобильных устройств.
5. Угрозы, связанные с мобильными приложениями.
6. Контроль установки и обновления приложений.
7. Аутентификация и авторизация пользователей мобильных устройств.
8. Биометрическая защита мобильных устройств.
9. Методы защиты данных на мобильных устройствах.
10. Шифрование информации на мобильных устройствах.
11. Безопасность хранения персональных данных.
12. Угрозы беспроводных интерфейсов мобильных устройств.
13. Защита при работе в публичных беспроводных сетях.
14. Безопасность мобильных платежей.
15. Защита корпоративных данных в мобильной среде.
16. Политики безопасности мобильных устройств.
17. Системы управления мобильными устройствами (MDM).
18. Контроль и мониторинг безопасности мобильных устройств.
19. Резервное копирование и восстановление данных.
20. Реагирование на инциденты мобильной безопасности.
21. Удалённое блокирование и стирание данных.
22. Аудит безопасности мобильных устройств.
23. Нормативные требования к безопасности мобильных устройств.
24. Интеграция мобильной безопасности в систему ИБ организации.
25. Роль специалиста по ИБ в обеспечении мобильной безопасности.

САМОСТОЯТЕЛЬНЫЕ ЗАДАНИЯ

Задание 1 Разработать электронную форму документа «Журнал учёта инцидентов информационной безопасности» (дата, тип инцидента, объект защиты, описание, уровень критичности, ответственный, статус).

Задание 2 Разработать электронную форму документа «Справочник угроз информационной безопасности» (наименование угрозы, источник, тип угрозы, возможные последствия, уровень риска).

Задание 3 Разработать электронную форму документа «Акт регистрации нарушения требований информационной безопасности» (дата, подразделение, сотрудник, описание нарушения, принятые меры, ответственное лицо).

Задание 4 По разработанным электронным формам документов спроектировать базу данных обеспечения информационной безопасности организации и реализовать её на ПЭВМ с использованием языка SQL (создание таблиц, ограничений целостности, связей).

Задание 5 Для разработанной базы данных сформировать SQL-запросы, обеспечивающие: выборку инцидентов за период, анализ инцидентов по типам угроз, отчёт по подразделениям, выявление наиболее критичных угроз поиск нарушений по сотруднику.

Задание 6 Для разработанной базы данных определить функциональные зависимости между атрибутами основных таблиц (инциденты, угрозы, сотрудники, подразделения).

Задание 7 Для разработанной базы данных определить потенциальные ключи и выбрать из них первичные и внешние ключи, обосновав их использование с точки зрения обеспечения целостности и безопасности данных.

Задание 8 Выполнить нормализацию базы данных (до 3-й нормальной формы), обосновав устранение избыточности и повышение надёжности хранения данных информационной безопасности.

ЭКЗАМЕНАЦИОННЫЕ (КОНТРОЛЬНЫЕ) ВОПРОСЫ

1. Понятие безопасности мобильных устройств.
2. Особенности мобильных устройств как объектов защиты.
3. Основные угрозы мобильной безопасности.
4. Классификация угроз безопасности мобильных устройств.
5. Источники мобильных угроз.
6. Риски, связанные с потерей и кражей мобильных устройств.
7. Мобильные операционные системы.
8. Уязвимости операционной системы Android.
9. Уязвимости операционной системы iOS.
10. Мобильные вредоносные программы.
11. Классификация мобильного вредоносного ПО.
12. Каналы распространения мобильных угроз.
13. Безопасность мобильных приложений.
14. Угрозы при установке сторонних приложений.
15. Контроль источников установки приложений.
16. Аутентификация пользователей мобильных устройств.
17. Авторизация и управление доступом.
18. Типовые ошибки реализации контроля доступа.
19. Биометрические методы защиты мобильных устройств.
20. Надёжность и ограничения биометрической аутентификации.
21. Риски применения биометрических технологий.
22. Защита данных, хранящихся на мобильных устройствах.
23. Шифрование памяти мобильных устройств.
24. Управление ключами шифрования.
25. Защита персональных данных на мобильных устройствах.
26. Конфиденциальность пользовательской информации.
27. Угрозы утечки данных с мобильных устройств.
28. Безопасность беспроводных интерфейсов мобильных устройств.
29. Угрозы при использовании Wi-Fi и Bluetooth.
30. Методы защиты беспроводных соединений.
31. Использование мобильных устройств в публичных сетях.
32. Риски работы в открытых беспроводных сетях.
33. Способы защиты при работе вне корпоративной сети.
34. Безопасность мобильных платежей.
35. Угрозы финансовой информации на мобильных устройствах.
36. Методы защиты мобильных транзакций.
37. Политики безопасности мобильных устройств.
38. Требования к использованию мобильных устройств в организации.
39. Контроль соблюдения политик мобильной безопасности.
40. Системы управления мобильными устройствами (MDM).
41. Основные функции и задачи MDM.
42. Применение MDM в корпоративной среде.
43. Концепция BYOD и её риски.
44. Меры защиты при использовании BYOD.
45. Разграничение личных и корпоративных данных.
46. Контейнеризация данных на мобильных устройствах.
47. Принципы разделения данных.
48. Преимущества контейнерного подхода.
49. Обновление программного обеспечения мобильных устройств.
50. Угрозы использования устаревшего ПО.
51. Управление обновлениями и патчами безопасности.
52. Резервное копирование данных мобильных устройств.
53. Восстановление данных после инцидентов.
54. Защита резервных копий мобильных данных.

55. Удалённое управление мобильными устройствами.
56. Блокирование и удалённое стирание данных.
57. Реагирование на потерю или кражу устройства.
58. Мониторинг безопасности мобильных устройств.
59. Журналирование событий мобильной безопасности.
60. Анализ инцидентов мобильной безопасности.
61. Аудит безопасности мобильных устройств.
62. Методы оценки защищённости мобильной среды.
63. Документирование результатов аудита.
64. Нормативно-правовые требования к безопасности мобильных устройств.
65. Требования по защите персональных данных.
66. Ответственность за нарушения мобильной безопасности.
67. Интеграция мобильной безопасности в систему ИБ организации.
68. Управление рисками мобильной безопасности.
69. Оценка эффективности мер защиты.
70. Социальная инженерия и мобильные угрозы.
71. Фишинг и SMS-мошенничество.
72. Методы противодействия социальным атакам.
73. Современные угрозы мобильной безопасности.
74. Тенденции развития мобильных атак.
75. Перспективы развития средств защиты мобильных устройств.

БИЛЕТЫ

ДЛЯ ПРОМЕЖУТОЧНОГО КОНТРОЛЯ ЗНАНИЙ ПО ДИСЦИПЛИНЕ (ДЛЯ ЗАЧЕТА – ПРОМЕЖУТОЧНАЯ АТТЕСТАЦИЯ)

МОУ ВО РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Факультет Естественнонаучный

Кафедра Информатики и ИТ

по « Безопасность WEB-приложений»

для 10.03.01 «Информационная безопасность»

профиль: Безопасность компьютерных систем

(по отрасли или в сфере профессиональной деятельности)

очная

Билет № 1

1. Роль специалиста по ИБ в обеспечении безопасности WEB-приложений.
2. Безопасная разработка WEB-приложений (Secure SDLC).

Утверждено на заседании кафедры _

протокол № 4 от «16» Ноября 2026г.

Заведующий кафедрой/_____/ Лешукович А.И.

Итоговые оценки студентов

Буквенное обозначение итоговых оценок студентов и их цифровые эквиваленты:

Буквенная оценка	Цифра	Общий балл	Традиционная оценка
A	4	95≤A≤100	отлично
A-	3,67	90≤A-<95	
B+	3,33	85≤B+<90	хорошо
B	3	80≤B<85	
B-	2,67	75≤B-<80	
C+	2,33	70≤C+<75	удовлетворительно
C	2	65≤C<70	
C-	1,67	60≤C-<65	

D+	1,33	55≤D+<60	
D	1	50≤D<55	
Fx	0	45≤Fx<50	неудовлетворительно
F	0	0<F<45	

Критерии выведения итоговой оценки промежуточной аттестации:

«Отлично» - средняя оценка ≥ 3,67.
«Хорошо» - средняя оценка ≥ 2,67 и ≤ 3,33.
«Удовлетворительно» - средняя оценка ≥ 1,0 и ≤ 2,33.
«Неудовлетворительно» - средняя оценка < 0.